eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Crawlers**
  - ✓ Definição
  - ✓ Utilizando ferramentas
  - ✓ Entendendo pastas ocultas
- ✓ **Scanners**
  - ✓ Definição
  - ✓ Scanners específicos: Wordpress
  - ✓ Scanners específicos: Joomla
  - ✓ Scanners específicos: Microsoft

Web Crawlers

Web Crawlers

Web crawler, em português rastreador web, é um programa de computador que navega pela internet de uma forma metódica e automatizada. Outros termos para Web crawlers são indexadores automáticos, bots, web spiders, Web robot, ou Web scutter.

O processo que um Web crawler executa é chamado de Web crawling ou spidering. Muitos sites, em particular os motores de busca, usam crawlers para manter uma base de dados atualizada.

Os Web crawlers são principalmente utilizados para criar uma cópia de todas as páginas visitadas para um pós-processamento por um motor de busca que irá indexar as páginas baixadas para prover buscas mais rápidas.

Crawlers também podem ser usados para tarefas de manutenção automatizadas em um Web site, como checar os links ou validar o código HTML. Os crawlers também podem ser usados para obter tipos específicos de informação das páginas da Web, como minerar endereços de email (mais comumente para spam).

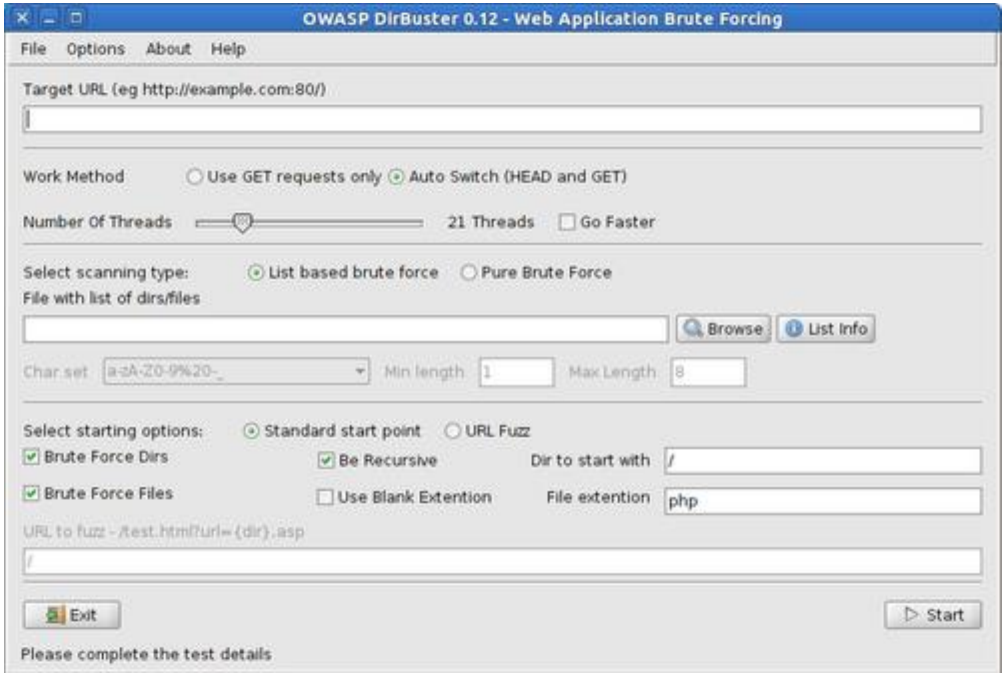
Web Crawlers

Um Web crawler é um tipo de robô de Internet ou agente de software.

Em geral, ele começa com uma lista de URLs para visitar (também chamado de seeds). À medida que o crawler visita essas URLs, ele identifica todos os links na página e os adiciona na lista de URLs para visitar. Tais URLs são visitadas recursivamente de acordo com um conjunto de regras.

Fonte: Wikipedia

Crawlers: Dirbuster



Crawlers: Dirbuster

DirBuster é uma aplicação feita em Java para descobrir nomes de diretórios e arquivos presentes em um site ou servidor usando brute force. Com isso, torna-se mais fácil a busca por algum diretório específico, facilitando a busca por dados ou diretórios que deveriam ser sigilosos.

O DirBuster tenta encontrar todos os diretórios e arquivos do site alvo.

No entanto, ferramentas dessa natureza são muitas vezes listadas com arquivos e diretórios comuns (padrões, exemplo: /admin/login.php).

DirBuster vem com um total de 9 listas diferentes, isto faz DirBuster extremamente eficaz para encontrar os arquivos e diretórios ocultos, ou que não seguem um padrão.

E se isso não fosse suficiente, DirBuster também tem a opção de realizar uma força bruta pura, o que deixa os diretórios e arquivos ocultos sem onde se esconder.

Crawlers: Dirbuster

O DirBuster oferece os seguintes recursos:

- Multi-threaded é possível efetuar mais de 6.000 solicitações por segundo.
- Analisa sites HTTP e HTTPS.
- Verificar a existência de diretórios e arquivos.
- Capaz de executar uma lista de verificação de força bruta baseado em uma wordlist ou pura.
- DirBuster pode ser iniciado em qualquer diretório.
- Cabeçalhos HTTP personalizados podem ser adicionados.
- Suporte a proxy.
- Extensões de arquivos personalizados podem ser usados.
- O desempenho pode ser ajustado durante o programa em execução.
- Suporta Basic, Digest e NTLM auth.
- Pode ser executado por linha de comando ou interface gráfica.

Crawlers: Dirbuster

DirBuster vem com um conjunto de listas únicas de diretórios e arquivos, estas foram geradas com base no arquivo e diretório de nomes que sejam efectivamente utilizadas por desenvolvedores de sites da internet.

A ordem das listas é baseado na frequência do item encontrado. Portanto, os itens mais comuns aparecem no topo.

directory-list-2.3-small.txt - (87650 palavras) - Directories/files que, são encontradas em pelo menos 3 hosts diferentes.

directory-list-2.3-medium.txt - (220546 palavras) - Directories/files que, são encontradas em pelo menos 2 hosts diferentes.

directory-list-2.3-big.txt - (1273819 palavras) - Todos directories/files que foram encontrados.

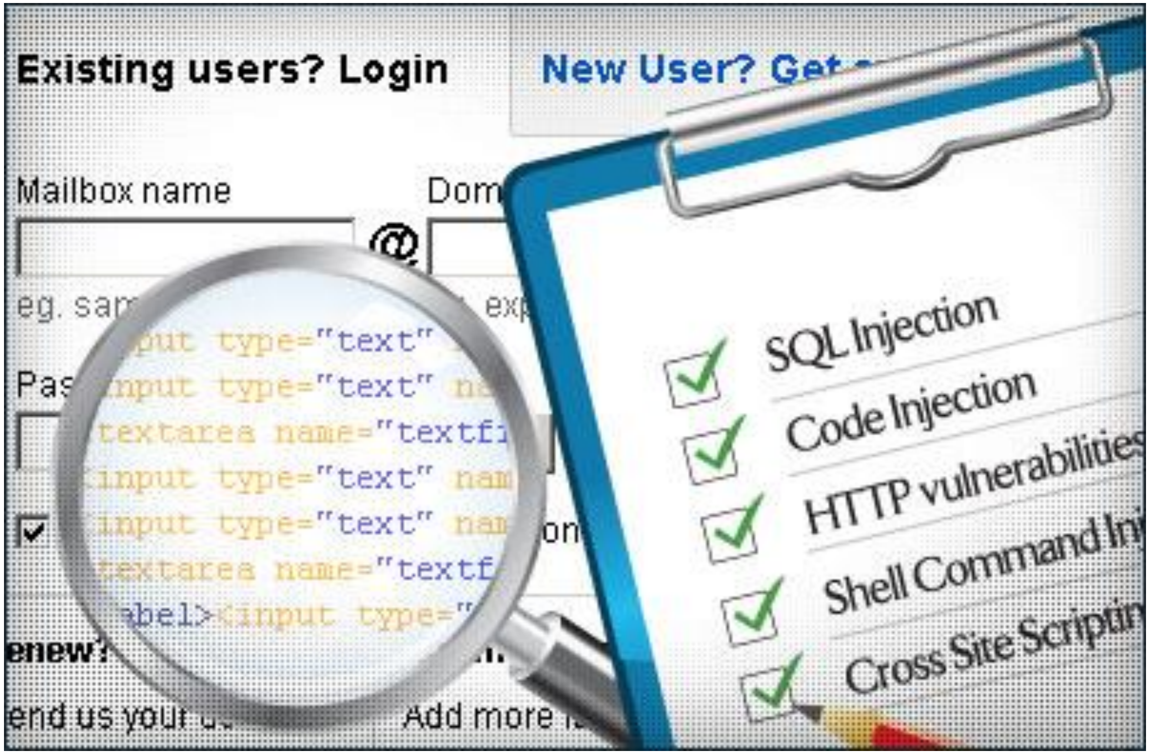
directory-list-lowercase-2.3-small.txt - (81629 palavras) - Case insensitive versão da lista directory-list-2.3-small.txt.

directory-list-lowercase-2.3-medium.txt - (207629 palavras) - Case insensitive versão da lista directory-list-2.3-medium.txt.

Crawlers: Dirbuster

directory-list-lowercase-2.3-medium.txt - (207629 palavras) - Case insensitive versão da lista directory-list-2.3-medium.txt.
directory-list-lowercase-2.3-big.txt - (1185240 palavras) - Case insensitive versão da lista directory-list-2.3-big.txt.
directory-list-1.0.txt - (141694 palavras) -Lista original sem ordem,organização específica.
apache-user-enum-1.0.txt - (8916 usernames) - Usado para adivinhar os usuários do sistema no Apache com o módulo userdir habilitado, com base em uma lista de nome de usuário (não ordenados).
apache-user-enum-2.0.txt - (10341 usernames) - Usado para adivinhar os usuários do sistema no Apache com o módulo userdir habilitado, com base em ~XXXXX encontrado durante a geração da lista (ordenada).

Scanners de Vulnerabilidades



Scanners de Vulnerabilidades

Um scanner de vulnerabilidades é um software que, dado um determinado alvo, seja ele um software, um computador ou um dispositivo de rede, irá analisá-lo em busca de vulnerabilidades existentes no alvo.

O scanner irá, sistematicamente, testar o alvo em busca de pontos vulneráveis a ataques (senhas padrão, serviços inseguros escutando em portas públicas, sistemas vulneráveis a falhas conhecidas, por exemplo).

Pode ser utilizado tanto para prevenção, na busca de falhas para correção, quanto para ataques, na identificação de vulnerabilidades acessíveis ao atacante.

Fonte: Wikipedia

Scanners: WPScan / JoomScan

Scanners: WPScan / JoomScan

Existem ferramentas específicas para varreduras em páginas como CMSs.

Essa ferramentas são úteis para empresas que trabalham com CMS, porém, não podemos dispensar as ferramentas mais robustas.

Busca padrão em sites Wordpress

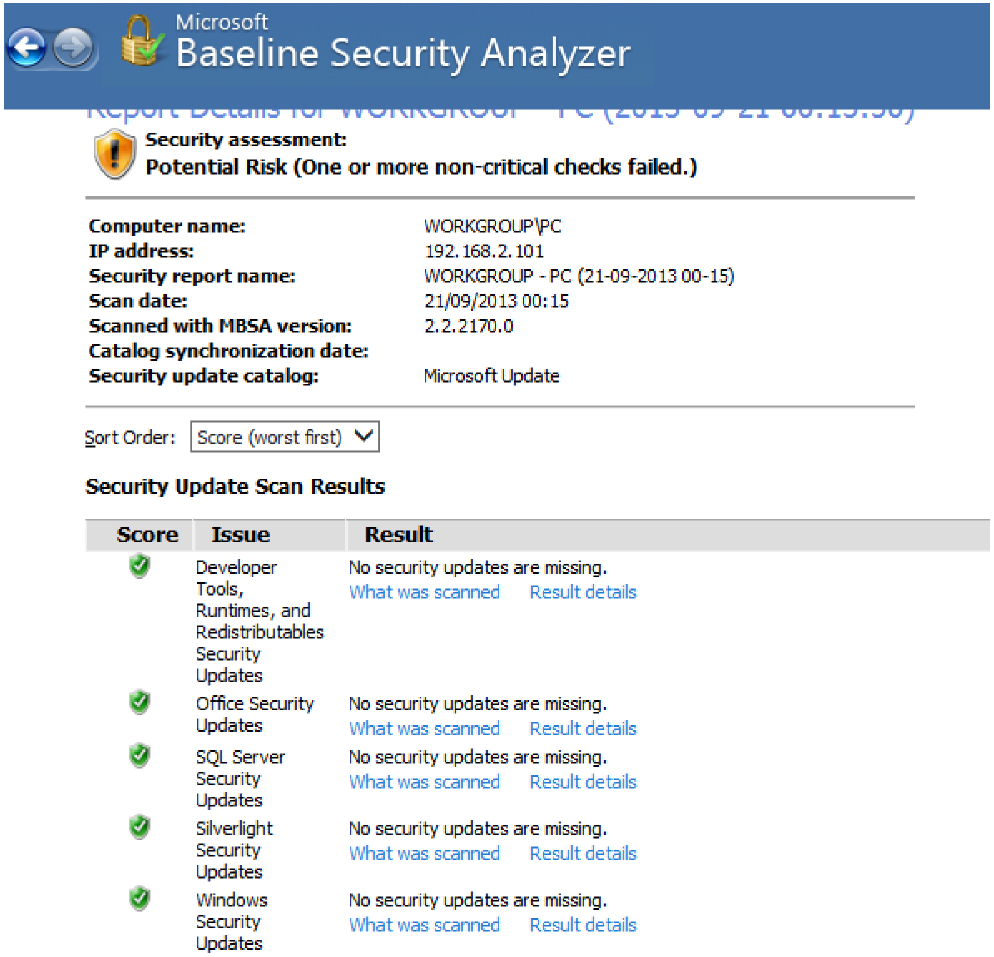
 # wpscan –url www.alvo.com

Busca padrão em sites Joomla

 # joomscan –u www.alvo.com

Scanners: MBSA

Scanners: MBSA



http://www.microsoft.com/en-us/download/details.aspx?id=7558

printf ("\Chega por hoje\n");

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker